#13 cw
6-14-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

JULIE A. GESCHWENDER et al.

Group Art Unit: 2164

Examiner: F. Poinvil

Serial No.: 09/425,471

Filed: October 22, 1999

For: SYSTEM AND METHOD FOR DETECTING PURCHASING CARD FRAUD

Attorney Docket No.: FDC 0136 PUS

APPEAL BRIEF UNDER 37 C.F.R. § 1.192

Box AF
Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231

Sir:

This is a brief in support of an appeal from the final rejection of claims 1-22, 24, and 27-30 in the final Office Action mailed on January 29, 2002.

I. Real Party In Interest

The real party in interest is First Data Corporation, a corporation organized and existing under the laws of the State of Delaware, and having a place of business at 401 Hackensack Avenue, Hackensack, New Jersey 07601.

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Box AF, Commissioner for Patents, U.S. Patent and Trademark Office, Washington, D.C. 20231 on:

May 21, 2002	James N. Kallis	
Date of Deposit	Name of Person Signing	Signature

II. Related Appeals and Interferences

There are no other appeals or interferences known to the Applicant, the Applicant's legal representative, or the Assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. Status of Claims

Claims 1-22, 24, and 27-30 are pending in this application (reproduced for reference in the attached Appendix) and are finally rejected and on appeal. Claims 1 and 14 are independent claims. Claims 2-13 and 27-28 depend directly or indirectly from independent claim 1. Claims 15-22, 24, and 29-30 depend directly or indirectly from independent claim 14.

IV. Status of Amendments

The Applicant proposed amendments to claims 1 and 14 in an Amendment after Final mailed on March 28, 2002, subsequent to the final Office Action. In the Advisory Action mailed on April 26, 2002, the Examiner indicated that the proposed amendments would be entered upon the timely submission of a Notice of Appeal and an Appeal Brief. The Applicant has filed a Reply after Final herewith cancelling the proposed amendments to claims 1 and 14 as the Applicant does not want the proposed amendments to be entered. The Applicant believes that the claims are already in a proper form for appeal without the proposed amendments. As such, the claims reproduced in the attached Appendix do not include the proposed amendments.

V. Summary of Invention

As generally described on page 4, line 11 through page 7, line 3 and FIGS. 1-4 of the Applicant's specification, the claimed invention is a method and system for detecting purchasing card fraud during all phases of a purchasing card life cycle. The

claimed invention includes obtaining contact event information from a client (20) during a contact event (18) (see step (50) in FIG. 2). As shown in FIG. 3, contact events (18) include: 1) application processing; 2) card activation; 3) cardholder usage including mail and telephone orders; and 4) maintenance events such as names and address changes and PIN changes.

The contact event information is then compared with fraud information used in known frauds and stored in a database (10) to determine if there is a fraud match between the contact event information and the fraud information (see step (52) in FIG. 2). The database (10) generally stores personal information used in known frauds. (See col. 2, lines 19-25; and col. 5, line 25 through col. 6, line 2. A fraud alert is then sent to the client (20) if there is a fraud match between the contact event information and the fraud information (see step (54) in FIG. 2).

VI. Issue

The Examiner finally rejected claims 1-22, 24, and 27-30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,819,226 issued to Gopinathan ("Gopinathan") in view of dialog file 148, accession no. 07947406 of Schott ("Schott").

The issue on appeal is whether Gopinathan in view of Schott makes a *prima facie* showing of obviousness of claims 1-22, 24, and 27-30.

VII. Grouping of Claims

Claims 1-22, 24, and 27-30 stand or fall together.

VIII. Argument

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references

themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success.

Finally, the prior art reference must teach or suggest all the claim limitations. MPEP 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is non-obvious under 35 U.S.C. § 103, then any claim depending therefrom is non-obvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

1. Background of the Claimed Invention

As described in the Background Art section of the Applicant's specification, purchasing card fraud could effectively be addressed through use of known fraudulent information such as known fraudulent names, known fraudulent addresses, known fraudulent phone numbers, etc.

2. The Claimed Invention

The claimed invention, as recited in independent claims 1 and 14, provides a method and system for detecting purchasing card fraud during all phases of a purchasing card life cycle. The claimed invention includes obtaining contact event information from a client during a purchasing card application process. The contact event information is then compared with fraud information used in known frauds and stored in a database to determine if there is a fraud match between the contact event information and the fraud

information. A fraud alert is then sent to the client if there is a fraud match between the contact event information and the fraud information.

3. Gopinathan and Schott

In the final Office Action, the Examiner posited that Gopinathan discloses a fraud detection system using predictive modeling. The system includes a computer database for receiving contact event information from a client, a computer software in communication with the computer database for comparing the contact event information with information stored in the database, and a communication network for informing the client that a fraud match has occurred. The Examiner cited col. 3, line 27 through col. 7, line 60; and col. 27, line 48 through col. 28, line 24 of Gopinathan.

The Examiner posited that Schott teaches methods to prevent purchasing card fraud in relation to usage or activation of a purchasing card. The Examiner cited the entire article of Schott and particularly page 4 of Schott. In the Advisory Action, the Examiner posited that Schott teaches a purchasing card application process whereby a caller calls an issuer which in turn accesses several sources to confirm and link the identity of the caller with the card before the card is activated. The Examiner noted page 2 of Schott for this teaching.

4. The Claimed Invention as Compared to Gopinathan and Schott

The claimed invention is different than any combination of Gopinathan and Schott in that the obtained contact information is compared with fraud information used in known frauds. As described on page 3, lines 19-25 and page 5, lines 25-27 of the Applicant's specification, known fraud information may include personal information such as addresses, telephone numbers, and social security numbers used in known frauds.

In the Response to Arguments section of the final Office Action, the Examiner responded to this argument by positing that Gopinathan discloses comparing

contact information with fraud information used in known frauds (citing col. 28, lines 3-15; col. 27, lines 3-15 and lines 48-63; and col. 6, lines 14-17 of Gopinathan).

Col. 28, lines 3-15 of Gopinathan disclose obtaining a fraud score using profile data summarizing known transactional patterns for a customer. For instance, these transactional patterns may indicate that the customer typically dines at low cost establishments as opposed to high priced restaurants. Col. 27, lines 3-15 and 48-63 of Gopinathan disclose a database having information from three sources: 1) general information on the customer; 2) data on all approved or declined previous transactions; and 3) a profile record which contains data describing the customer's transactional pattern. As such, none of these cited portions of Gopinathan teach or suggest using fraud information used in known frauds to determine if there is a fraud match between contact event information and the fraud information.

Col. 6, lines 14-17 of Gopinathan recites a fraud database which indicates which accounts had fraudulent activity and when the fraudulent activity occurred. Accordingly, the fraud database of Gopinathan identifies which accounts had fraudulent activity and when the fraudulent activity occurred as opposed to storing fraud information (i.e., known fraudulent names, known fraudulent addresses, etc.) used in known frauds. That is, the fraud database of Gopinathan tags and dates accounts having fraudulent activity as opposed to storing fraud information such as fraudulent personal information used in performing a fraudulent activity.

Schott discloses fraud scorecards and fraud detection software on page 4. Schott does not disclose whether the fraud scorecards and the fraud detection software uses fraud information known in used frauds. Schott discloses on pages 6-7 a national database in which purchasing card applications should be screened to prevent fraud. However, Schott does not teach or suggest whether this national database stores fraudulent information used in known frauds. For instance, such national databases store a purchasing card applicant's credit rating information which is not fraudulent information used in known frauds.

Further, this national database is disclosed as being used for purchasing card applications which may involve different considerations than other purchasing card contact events such as cardholder usage. These different considerations could be addressed by using fraud information used in known frauds as recited by the claimed invention.

Accordingly, independent claims 1 and 14 patentably distinguish over any combination of Gopinathan and Schott. Claims 2-13, 15-22, 24, and 27-30 depend from one of independent claims 1 and 14 and include all of the limitations therein. Thus, claims 1-22, 24, and 27-30 patentably distinguish over any combination of Gopinathan and Schott.

IX. Summary

Claims 1-22, 24, and 27-30 are patentable for the reasons discussed above.

Respectfully submitted,

JULIE A. GESCHWENDER et al.

By_____

James N. Kallis
Reg. No. 41,102
Attorney for Applicant

Date: May 21, 2002

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351

APPENDIX

1. A method for detecting purchasing card fraud during all phases of a purchasing card life cycle, the method comprising:

obtaining contact event information from a client during a contact event;

comparing the contact event information with fraud information used in known frauds and stored in a database to determine if there is a fraud match between the contact event information and the fraud information; and

sending a fraud alert to the client if there is a fraud match between the contact event information and the fraud information.

2. The method of claim 1 wherein obtaining contact event information further comprises obtaining a customer's name, social security number, and address.

3. The method of claim 1 further comprising receiving the fraud information at the database from a plurality of fraud information sources.

4. The method of claim 1 wherein obtaining contact event information further comprises obtaining contact event information during a purchasing card application process.

5. The method of claim 1 wherein obtaining contact event information further comprises obtaining contact event information during a purchasing card activation process.

6. The method of claim 1 wherein obtaining contact event information further comprises obtaining contact event information during a purchasing card mail order transaction from a retail participant.

7. The method of claim 1 wherein obtaining contact event information further comprises obtaining contact event information during a purchasing card phone order transaction.

8. A method of claim 1 wherein obtaining contact event information further comprises obtaining contact event information during an address change process.

9. The method of claim 1 wherein sending a fraud alert further comprises sending an account record to an online queue to be monitored by the client.

10. The method of claim 9 wherein sending an account record further comprises suspending the contact event until a manual follow-up is completed.

11. The method of claim 1 further comprising scoring the fraud match to assist in the fraud determination process.

12. The method of claim 11 wherein scoring the fraud match further comprises predicting a likelihood of a fraudulent takeover of a cardholder account.

13. The method of claim 1 further comprising suspending purchasing card generation when a fraud match occurs.

14. A system for detecting purchasing card fraud during all phases of a purchasing card life cycle, the system comprising:

a computer database for receiving contact event information from a client;

computer software in communication with the computer database for comparing the contact event information with fraud information used in known frauds and stored in the database to determine if there is a fraud match between the contact event information and the fraud information; and

a communication network in communication with the database for sending a fraud alert to the client if there is a fraud match between the contact event information and the fraud information.

15. The system of claim 14 wherein the contact event information comprises a customer's name, social security number, and address.

16. The system of claim 14 wherein the fraud database is adapted to communicate with a plurality of fraud information sources.

17. The system of claim 14 wherein the computer database receives the contact event information during a purchasing card application process.

18. The system of claim 14 wherein the computer database receives the contact event information during a purchasing card activation process.

19. The system of claim 14 wherein the computer database receives the contact event information during a purchasing card mail order transaction from a retail participant.

20. The system of claim 14 wherein the computer database receives the contact event information during a purchasing card phone order transaction.

21. The system of claim 14 wherein the computer database receives the contact event information during an address change process.

22. The system of claim 14 wherein the fraud alert includes an account record which is sent to an online queue monitored by the client.

24. The system of claim 14 wherein the computer software is operative to score the fraud match to assist in the fraud determination process.

27. The method of claim 1 wherein the sending step includes sending the fraud alert in real time.

28. The method of claim 1 wherein the sending step includes sending the fraud alert via batch.

29. The system of claim 14 wherein the computer software and the communication network are operative to send the fraud alert in real time.

30. The system of claim 14 wherein the computer software and the communication network are operative to send the fraud alert via batch.